AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: WILLIAM FARRIOR

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)
(Briefly describe the property to be search)
Or identify the person by name and address))
INFORMATION ASSOCIATED WITH:) Case No: M-20-143-SM
stevenmgrdichian@gmail.com,)
morganscatering52@gmail.com,)
desrocher11@gmail.com,)
goldstyles123@gmail.com, and)
pinkmansionrenovations@gmail.com,)
THAT IS STORED AT PREMISES CONTROLLED BY:)
GOOGLE, INC.)
1600 Amphitheatre Parkway,)
Mountain View, California 94043)

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030	Computer Fraud
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1344	Bank Fraud

The application is based on these facts:

See attached Affidavit of Special Agent Timothy Mark Bragg, Federal Bureau of Investigation, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Timothy Mark Bragg
Digitally signed by Timothy Mark Bragg
Date: 2020.04.02 11:21:42 -05'00'

Applicant's signature

TIMOTHY MARK BRAGG
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: April 2, 2020

Judge's signature

City and State: Oklahoma City, Oklahoma

SUZANNE MITCHELL, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Timothy Mark Bragg, being duly sworn, depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since approximately March 2009. I am currently assigned to the FBI's Oklahoma City Field Office, Stillwater Resident Agency. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to computer intrusion and internet fraud. As a result of my training and experience, including information provided by other federal agents with applicable knowledge, I am familiar with the tactics, methods, and techniques utilized by online fraud rings and their members. As part of my job, I have conducted numerous investigations involving the use of the Internet, email, and social media to further criminal activity. I have participated in the execution of multiple federal search warrants involving various types of evidence and property.

2. This affidavit is made in support of an application for a search warrant for content and records associated with the electronic mail ("email") accounts **stevenmgrdichian@gmail.com, morganscatering52@gmail.com, desrocher11@gmail.com, goldstyles123@gmail.com, and pinkmansionrenovations@gmail.com** ("target email accounts") that is stored at premises controlled by Google, LLC ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched and seized is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of information (including the content of communications) further described

in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons (to include members of the FBI and the United States Attorney's Office in the Western District of Oklahoma) will review that information to locate the items described in Section II of Attachment B.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have set forth only the facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030 (Computer Fraud and Abuse Act), § 1341 and § 1343 (Mail and Wire Fraud), and § 1344 (Bank Fraud), are presently located in the content and records associated with the target email accounts. This affidavit is based on my personal observations, my training and experience, and information obtained from other agents and witnesses.

4. My investigation has focused on a complex fraud scheme, perpetrated by yet to be identified subject(s), which targeted the Oklahoma State University Athletic Department (hereinafter, "OSU Athletic Department") and the Oklahoma State University Foundation (hereinafter, "The Foundation"). The target(s) of the investigation used fraudulent and/or stolen credit cards to purchase athletic event tickets (which included associated fees and required donations to The Foundation), via online ticket marketplace, Ticketmaster, from Oklahoma State University. The fraud scheme resulted in a realized loss to both the OSU Athletic Department and The Foundation totaling $689,880.89.[1] The investigation has revealed that there is probable cause to believe that the content and records associated with the target email accounts, which are

[1] Total realized loss of $689,880.89 includes a loss of $309,020.03 from The Foundation and $380,860.89 from the OSU Athletic Department. Aggregate loss totals provided to the Federal Bureau of Investigation (FBI) by the Oklahoma State University A&M Board of Regents Office of Internal Audit and is accurate as of March 11, 2020.

maintained by Google, contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1030, 1341, 1343, and 1344, among others. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

BACKGROUND CONCERNING EMAIL AND GOOGLE

5. Based on my training, experience, and knowledge, as well as information provided to me by other law enforcement agents, I know the Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. To access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The worldwide web ("www") is a functionality of the Internet that allows users of the Internet to share information.

6. With a computer connected to the Internet, an individual computer user can make electronic contact with computers and other electronic devices around the world. This connection can be made by any means, including modem, local area network, wireless, and numerous other methods.

7. Email is a popular form of electronically transmitting messages and files between computer users. When an individual computer user sends an email, it is initiated at the user's computer (including, for example, an iPhone or iPad), transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

8. In general, an email that is sent to an email subscriber is stored in the subscriber's "mail box" on the email provider's servers until the subscriber deletes the email. If the

subscriber does not delete the message, the message can remain on the provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the provider's servers for a period of time.

9. In my training and experience, I have learned that Google provides a variety of on-line services, including email access, to the public. Google allows subscribers to obtain email accounts at the domain name Gmail.com like the target email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google requests subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

10. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, chat history, pictures via a linked Google Picasa account (other than ones attached to emails), bookmarks, and other files such as those stored in linked Google Documents and Google Drive applications, on servers maintained and/or owned by Google. Google also stores search terms entered into Google Search tool by a user who is simultaneously logged into their Google e-mail account. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures, files, and search terms.

11. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, such information may constitute evidence of the crimes under investigation because even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

12. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

13. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as

technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*,

location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

15. Google offers a service called G Suite, which offers businesses additional services beyond what comes with Google's free consumer applications. These include custom business email addresses using your company's domain (e.g., xxx@company.com), additional cloud storage for email, and other services. G Suite also integrates with other Google services including Calendar, Google Drive, Hangouts, Blogger, and more. Google stores the company's emails and associated records on its servers.

JURISDICTION

16. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

THE RELEVANT FACTS

17. The FBI and the United States Attorney's Office of the Western District of Oklahoma are currently investigating a fraud scheme perpetrated by yet to be identified subject(s), which targeted the OSU Athletic Department and The Foundation resulting in realized loss totaling $689,880.89.

18. Upon notification by the OSU Athletic Department Ticketing Office ("Ticketing Office") of multiple charge backs for the purchase of athletic event tickets, the Oklahoma State University A&M Board of Regents Office of Internal Audit ("Audit Office") conducted an audit of the purchase activity associated with the identified charge backs. This audit identified multiple unique Ticketmaster accounts, with associated account names and email addresses, which used multiple credit cards to purchase tickets to Oklahoma State Football and Oklahoma State Men's Basketball games. A subset of the total ticket purchases included 1,086 tickets to the 2019 Oklahoma State University versus University of Oklahoma football game ("Bedlam"). These tickets were purchased by the below identified unique Ticketmaster accounts:

Bedlam Fraudulent Ticket Purchase Totals

Account ID	Account Name	Account Email	Total Tickets Purchased
2332515	David Kominsky	additionalcorp1@gmail.com	2
2332613	Bonnie Llos	larrymoving@aol.com	20
2332690	Cathy Grangien	catering12345@aol.com	9
2332661	Dave Lase	sean_cohen@aol.com	4
2333657	Deborah Rocher	**desrocher11@gmail.com**	57
2332571	Doop Fokus	manner12345@aol.com	15
2332936	James Li	**morganscatering52@gmail.com**	191
2332807	James Norman	**goldstyles123@gmail.com**	70
2332655	Jarry Wright	bonniebon64@yahoo.com	55
2333550	Jason Morgan	thecomputer1920@yahoo.com	17
2332843	Patrick Mover	patricksmoving@aol.com	172
2332758	Peter Morris	citywideinstallers@yahoo.com	32
2334043	Tommy Loos	**pinkmansionrenovations@gmail.com**	442

19. The Audit Office identified secondary ticket market company, Tickets For Less, as a company that sold a portion of the fraudulently purchased Bedlam tickets to retail customers. The FBI interviewed Clay Discher, Vice President of Purchasing for Tickets For Less. Tickets For Less sold 1,290 tickets to the 2019 Bedlam game. I cross-referenced the Bedlam game tickets that Tickets For Less sold against the list of fraudulently purchased tickets provided by the Audit Office, and identified 155 tickets that were fraudulently purchased tickets.

Per Discher, a portion of Tickets For Less's total Bedlam game ticket sales of 1,290 were originally purchased by Tickets For Less from ticket market company, Ticket Network. Discher stated that, sometime before the Bedlam game, he noticed a large amount of Bedlam tickets being listed for sale for approximately 50% of the market price, by secondary ticket market company Ticket Network.

20. Ticket Network serves as a broker between buyers and sellers on the secondary ticket market, and as such, despite the fact that Tickets For Less purchased a portion of the Bedlam game tickets through Ticket Network, Ticket Network is not the seller of the tickets. I provided Ticket Network with a list of the aforementioned 155 tickets (identified by event name, section, row, number of seats, and seat numbers) sold by Tickets For Less, and which were a part of the 1,086 fraudulently purchased tickets and asked if they brokered the sale to Tickets For Less. Because Ticket Network does not track their ticket inventory to the specific seat number, rather it tracks all inventory identified by event name, section, row, and number of seats listed for sale, Ticket Network could not confirm that the specific 155 tickets passed through its company. However, Ticket Network identified Steven Mgrdichian ("Mgrdichian") as a broker who listed 49 tickets for sale to the Bedlam football game, which map to some of the same sections, rows, and number of seats as those in the list of 155 fraudulent tickets sold to retail customers by Tickets For Less.

21. Ticket Network provided the FBI records depicting all inventory that Mgrdichian listed for sale on Ticket Network from November 1 through November 30, 2019. These records showed that Mgrdichian's inventory of Bedlam game tickets, listed for sale with Ticket Network, included a total of 68 tickets on November 29, 2019, and a total of 231 tickets on November 30, 2019. A cross-reference of Mgrdichian's Bedlam game tickets inventory with Ticket Network

against the list of total number of fraudulently purchased tickets provided by the Audit Office identified 270 tickets which map to some of the same sections, rows, and range of number of seats as those in the list of total number of fraudulently purchased tickets provided by the Audit Office. Specifically, Mgrdichian's inventory mapped to the section, row, and range of number of seats of four of the 57 tickets fraudulently purchased by Rocher (desrocher11@gmail.com), 84 of the 191 tickets fraudulently purchased by Li (morganscatering52@gmail.com), 63 of 70 tickets fraudulently purchased by Norman (goldstyles123@gmail.com), two of the 172 tickets fraudulently purchased by Mover (patricksmoving@aol.com), and 117 of 442 tickets fraudulently purchased by Loos (pinkmansionrenovations@gmail.com).

22. My research indicates that these email addresses were created for the purpose of effecting this fraudulent scheme due to the fact that their respective creation dates are close to the dates of their initial fraudulent purchases.

Email Creation Date/First Fraudulent Purchase Date

Account Name	Account Email Address	Email Creation Date	Purchase Date
Rocher	desrocher11@gmail.com	11/28/2019	11/28/2019
Li	morganscatering@gmail.com	11/26/2019	11/29/2019
Norman	goldstyles123@gmail.com	11/19/2019	11/29/2019
Loos	pinkmansionrenovations@gmail.com	10/5/2019	11/30/2019
Mover	patricksmoving@aol.com	11/26/2019	11/27/2019

23. Ticket Network records show that Mgrdichian created an account with Ticket Network on October 31, 2018, under the company name "Steven Mgrdichian" with Mgrdichian listed as the owner. Mgrdichian's account with Ticket Network lists an address associated with "Steven Mgrdichian" as 98 Walker Drive, Brampton, Ontario, Canada L6T4H6, telephone number +1-647-532-6399, and email account address stevenmgrdichian@gmail.com. Open source research of "Steven Mgrdichian" failed to identify any event ticket brokering company in that name, nor did it identify any Canadian-based individual name Steven Mgrdichian. Open source research of 98 Walker Drive, Brampton, Ontario, Canada L6T4H6 lists Canadian

company, Empack Spraytech, Inc., as the owner of this address, which was corroborated by a Google Maps Street View image depicting an office building at this address with a sign reading "empack" on the front of the building. Additionally, the fact that this address was utilized to create Mgrdichian's account with Ticket Network in October 2018 reveals the attempt, by Mgrdichian, to hide the location of his company from the onset of his ticket brokering relationship with Ticket Network. My research suggests that Mgrdichian has been attempting to obfuscate his true identity, location, and nature of his business from October 2018 to present.

CONCLUSION

24. Accordingly, based on the above, the email accounts **stevenmgrdichian@gmail.com, morganscatering52@gmail.com, desrocher11@gmail.com, goldstyles123@gmail.com,** and **pinkmansionrenovations@gmail.com** are being used in the criminal scheme under investigation, and there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030 (Computer Fraud and Abuse Act), § 1341 and § 1343 (Mail and Wire Fraud), and § 1344 (Bank Fraud), will be found at Google in the content and records associated with the target email accounts.

25. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

BRAGG.TIMOTHY.M.F22M39K50
2020.04.02 11:33:25 -05'00'

Timothy Mark Bragg
Federal Bureau of Investigation

Subscribed and sworn to before me on April 2, 2020.

SUZANNE MITCHELL
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with all Google services associated with the accounts listed below (collectively referred to as the "target email accounts"), during the identified time period, including but not limited to email, chat communications, search history, contacts, calendar entries, Google Drive documents, bookmarks, Picasa Albums which is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

- **stevenmgrdichian@gmail.com**
  - **October 31, 2018 to present**
- **morganscatering52@gmail.com**
  - **November 26, 2019 to present**
- **desrocher11@gmail.com**
  - **November 28, 2019 to present**
- **goldstyles123@gmail.com**
  - **November 19, 2019 to present**
- **pinkmansionrenovations@gmail.com**
  - **October 5, 2019 to present**

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Google, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each of the five target email accounts listed in Attachment A:

a. All records or other information pertaining to the accounts of target email accounts, including all files, databases, and database records stored by Google in relation to that account or identifier;

b. All information in the possession of Google that might identify the subscribers related to the target email accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records pertaining to the types of service utilized by the target email accounts;

d. All records pertaining to communications between Google and any person regarding the target email accounts, including contacts with support services and records of actions taken;

e. All historical source-destination Internet Protocol ("IP") logs associated with the target email accounts from inception of target email accounts through the return date of this

warrant;

f. The contents of all e-mails associated with the target email accounts, including stored or preserved copies of e-mails sent to and from the account, draft e- mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail during the time period identified in Attachment 'A';

g. All search history and web history by the user of the target email accounts;

h. All records or other information stored at any time by an individual using the target email accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

i. For the target email accounts, provide the Android device information for each target email accounts, including IMEI/MEID, make and model, serial number, date and IP address of last access to Google, and a list of all accounts that have ever been active on the device;

j. All records (including content records) pertaining to any Google service associated with the target email accounts, including the following services:

1. Android
2. G Suite
3. Google AdSense
4. Google Calendar
5. Google Play
6. Google Services
7. Google Talk
8. Google Webmaster Tools
9. Google+
10. Location History
11. Picasa Web Albums
12. Web History
13. iGoogle
14. Google Drive
15. Blogger
16. Contacts
17. Google Analytics
18. Gmail

19. Google Cloud Print
20. Google Code
21. Google Dashboard
22. Google Developers Console
23. Google Chrome Sync
24. Google Docs
25. Google Mobile
26. Google Photos
27. Google Sites
28. Google Hangouts

k. All subscriber records, transactional information, search query history, browsing history, machine cookies, e-mail accounts ever linked to:

1. Google Maps location information
2. Google Location history
3. Face Unlock information (stored images)

Google is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitute fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 1030 (Computer Fraud and Abuse Act), § 1341 (Mail Fraud), § 1343 (Wire Fraud) and § 1344 (Bank Fraud), occurring between October 31, 2018, and the date of this warrant, including information pertaining to the following matters:

a. Records, documents, and information relating to the theft, trafficking, distribution, sale, or use of athletic event tickets;

b. Records, documents, and information relating to a scheme to defraud or obtain money or property from the OSU Athletic Department and/or The Foundation through false pretenses, representations, or promises with regard to the theft, trafficking, distribution, sale, or use of athletic event tickets;

c. Records, documents, and information relating to financial transactions involving the proceeds from the theft, trafficking, distribution, sale, or use of athletic event tickets, including but not limited to the promotion of such activities or the concealment of the nature, location, source, ownership, or control of the proceeds obtained from such activities;

d. References to athletic event ticket primary and secondary marketplace accounts, and changing email addresses, passwords, or other information associated with those accounts or otherwise using those accounts;

e. Records, documents, and information relating to the identity of individuals using the following names Tommy Loos, Peter Morris, Patrick Mover, Jason Morgan, Jarry Wright, James Norman, James Li, Doop Fokus, Deborah Rocher, Dave Lase, Cathy Grangien, Bonnie Llos, David Kominsky, and Steven Mgrdichian;

f. Records, documents, and information relating to who owns, controls, works at, or is associated with ticket broker company STEVEN MGRDICHIAN

g. Athletic event e-Tickets;

h. Email addresses or passwords for primary and secondary event ticket marketplaces;

i. Evidence indicating how and when the target email accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the target email accounts' owners;

j. Evidence indicating the states of mind of the users of the target email accounts, as it relates to the crimes under investigation; and

k. The identity of the person(s) who made payments through, received payments through, or otherwise communicated with or through the target email accounts in connection with the theft, trafficking, distribution, sale, or use of athletic event tickets, including records that help reveal their whereabouts.